

1                    INFORMATION PROCESSING WITH DATA STORAGE

2    FIELD OF INVENTION

3            The present invention relates to data encryption  
4 processing (encryption of write data and decryption of read  
5 data) in an external storage device (a data storage device)  
6 represented by a hard disk device.

7    BACKGROUND OF THE INVENTION

8            There are various external storage devices for a  
9 computer system such as magnetic disk devices (a hard disk  
10 drive and the like), optical disk devices, or memory cards  
11 using semiconductor memories. Various measures have been  
12 introduced to protect the data to be stored in these storage  
13 devices from the viewpoint of security. Among them, a  
14 password lock function is normally supported as a user  
15 verification function in a hard disk device in which a user  
16 frequently stores personal information. In the password  
17 lock function, a password set by the user is written in a  
18 special area of the hard disk, whereby the hard disk is  
19 operated to accept an access request if a password inputted  
20 upon starting up matches the previously written password, or  
21 refuses the access to the hard disk device if the passwords  
22 do not match each other.

23           Meanwhile, encryption of the data stored in the  
24 storage device (hereinafter referred to as the "stored  
25 data") is effective as means for protecting the stored data  
26 from an access by a third party. Conventionally, in the

1 case of encrypting the data to be stored in the storage  
2 device, such data has been encrypted before storing it in  
3 the storage device by use of encryption software or hardware  
4 provided in a computer device side (see Patent References 1  
5 and 2, for example).

6 (Patent Reference 1)

7 Japanese Unexamined Patent Publication No. 2002 -  
8 319230

9 (Patent Reference 2)

10 Japanese Unexamined Patent Publication No. 11 (1999) -  
11 352881

12 By use of the user verification such as the password  
13 lock and the encryption of the stored data at the same time  
14 as described above, it is possible to eliminate the risk of  
15 a theft of the contents of the stored data by a third party  
16 even if the user verification is unlocked by the third  
17 party. However, there is a problem happening as to how to  
18 provide a key to the encryption (hereinafter referred to as  
19 the "encryption key").

20 The length of the encryption key is usually 128 bits  
21 or longer, which is too long for the user to provide  
22 directly upon the encryption or the decryption of the stored  
23 data. On the contrary, the function of encryption will be  
24 lost if the encryption key is recorded and held in a record-  
25 ing medium. Accordingly, when the user verification and the  
26 encryption of the user data are used at the same time, one  
27 conceivable mode is to create the encryption key based on  
28 personal identification information (including the password)  
29 to be used for the verification. However, in this mode, the  
30 encryption key is changed every time when the personal  
31 identification information is changed periodically or at

1 random from the viewpoint of security. Accordingly, it is  
2 necessary to decrypt the data with the old encryption key,  
3 and to encrypt the stored data again with the new encryption  
4 key. Storage capacities of hard disk devices have been  
5 increasing in these days, and some of them may exceed 100  
6 gigabytes (GB). As a consequence, it will take a lot of  
7 time if re-encryption of the stored data is requested every  
8 time of changing the personal identification information,  
9 which is not deemed preferable.

10 Meanwhile, it is becoming more popular in these days  
11 to implement the hard disk device detachably (removably) on  
12 the computer device, so that the data are utilized by chang-  
13 ing the hard disk device or by setting the hard disk device  
14 to another computer device. When a data encryption function  
15 is implemented on the hard disk under such use  
16 circumstances, it is necessary to thoroughly consider on  
17 compatibility with a hard disk which does not include the  
18 encryption function. Here, preparation of a special command  
19 for initial setting upon execution of encryption is not a  
20 problem. However, in the implementation where a special  
21 command is also required for read/write processing upon data  
22 encryption, significant modification of a basic input/output  
23 system (BIOS) or an operating system (OS) is necessary for  
24 supporting such a command, which is not deemed preferable.

25 It is also possible to determine as to whether or not  
26 encryption of the stored data in the hard disk device is  
27 executed with the entire magnetic disk by means of setting  
28 jumper pins or by format options. However, many hard disk  
29 devices are built-in in computer devices recently and are  
30 shipped after pre-installation of the OS and other software.  
31 Accordingly, it is not possible to encrypt the data at this

1 initial state. It is because a secret key for encryption  
2 should be determined by each user and should be different in  
3 each disk.

4 In this case, there is also an option which is to turn  
5 off the encryption function upon the above-mentioned  
6 pre-installation of the software so as to allow the user who  
7 needs the encryption function to conduct encryption of the  
8 entire magnetic disk by himself. However, if the storage  
9 capacity of the magnetic disk is large, it takes a lot of  
10 time for the encryption processing of the entire magnetic  
11 disk. As a consequence, the burden on the user is  
12 increased.

13 Moreover, it is also possible to divide the storage  
14 area of the magnetic disk into an encrypted area and a  
15 non-encrypted area, and to write the preinstalled data in  
16 the non-encrypted area. However, modification of the system  
17 such as the OS becomes necessary for constantly monitoring  
18 to avoid the data from being transferred between the  
19 encrypted area and the non-encrypted area upon subsequent  
20 data reading or writing.

## 21 SUMMARY OF THE INVENTION

22 Accordingly, an aspect of the present invention is to  
23 achieve encryption processing of the stored data and manage-  
24 ment of an encryption key, which are suitable for the case  
25 when user verification and encryption of the stored data are  
26 applied to a storage device at the same time.

27 Another aspect of the present invention is to provide  
28 a method of encryption processing for the stored data

1 suitable for a detachably implemented storage device, and to  
2 provide a storage device which can achieve the method of  
3 encryption processing.

4 To attain the foregoing aspects, the present inven-  
5 tion is realized as a data storage device to be configured  
6 as follows. Specifically, the data storage device includes  
7 an encryption circuit for encrypting desired data and  
8 personal identification information by use of an encryption  
9 key created out of a given piece of the personal identifica-  
10 tion information such as a password; a recording medium for  
11 recording the data and the personal identification informa-  
12 tion which are encrypted by the encryption circuit, and a  
13 control unit for executing user verification by use of the  
14 encrypted personal identification information stored in the  
15 recording medium.

16 Still another aspect of the present invention for  
17 attaining the foregoing aspects is also realized as a data  
18 storage device configured as follows. Specifically, the  
19 data storage device includes a magnetic disk, a read-and-  
20 write mechanism for reading and writing data, and a control  
21 mechanism which has an encryption function for encrypting  
22 data to be written in the magnetic disk and for decrypting  
23 the encrypted data to be read out of the magnetic disk, and  
24 controls reading and writing of the data by the reading-and-  
25 writing mechanism.

26 Moreover, another data processing method according to  
27 the present invention includes the steps of creating an  
28 verification encryption key out of a given piece of personal  
29 identification information, encrypting the personal identi-  
30 fication information by use of the verification encryption  
31 key and thereby recording the encrypted personal

1 identification information in a recording medium as verifi-  
2 cation data while encrypting a data encryption key by use of  
3 the verification encryption key and thereby recording the  
4 encrypted data encryption key in the recording medium,  
5 executing user verification based on the verification data,  
6 decrypting the data encryption key by use of the verifica-  
7 tion encryption key, and encrypting write data transmitted  
8 from a host system by use of the decrypted data encryption  
9 key and thereby recording the encrypted write data in the  
10 recording medium or decrypting the data read out of the  
11 recording medium by use of the data encryption key and  
12 thereby transmitting the decrypted data to the host system.

#### 13 BRIEF DESCRIPTION OF THE DRAWINGS

14 For a more complete understanding of the present  
15 invention and the advantages thereof, reference is now made  
16 to the following description taken in conjunction with the  
17 accompanying drawings.

18 Fig. 1 is a view showing a configuration example of a  
19 hard disk device according to an embodiment of the present  
20 invention.

21 Fig. 2 is a view describing a method of initial  
22 setting of user verification according to the embodiment.

23 Fig. 3 is a view describing a method of the user  
24 verification and encryption processing of stored data  
25 according to the embodiment.

26 Fig. 4 is a view describing a method of restoring the  
27 stored data when a trouble occurs in a magnetic disk accord-  
28 ing to the embodiment.

1           Fig. 5 is a view describing a method of restoring the  
2 stored data by use of a master key according to the  
3 embodiment.

4           Fig. 6 is a view describing a method of setting  
5 verification data for canceling a lock of the hard disk  
6 device in addition to other verification data based on  
7 personal identification information.

8           Fig. 7 is a view describing a responding method for  
9 the encryption processing in a case of changing the personal  
10 identification information according to the embodiment,  
11 which describes an operation of initial setting.

12           Fig. 8 is another view describing the method for the  
13 encryption processing in the case of changing the personal  
14 identification information according to the embodiment,  
15 which describes the user verification and the encryption  
16 processing of the stored data.

17           Fig. 9 is a view describing an operation of changing  
18 the personal identification information according to the  
19 embodiment.

20           Figs. 10A and 10B are views describing a method of  
21 data recovery according to the embodiment.

22           Fig. 11 is a view describing a method of setting a  
23 data encryption key to be usable by anybody along with a  
24 release of the user verification according to the  
25 embodiment.

26           Fig. 12 is a view describing a method to recover the  
27 stored data by use of a master key when a verification  
28 encryption key and a data encryption key are separately  
29 provided in the embodiment.

30           Fig. 13 is a view showing the concepts of the encryp-  
31 tion and decryption processing in the ECB mode and the CBC

1 mode.

2 Fig. 14 is a view schematically showing a data  
3 configuration of a sector corresponding to the encryption  
4 processing according to the embodiment.

5 Fig. 15 is a view showing aspects of sector data and  
6 flag bits when data reading and writing is executed in the  
7 state of turning off an encryption function of the hard disk  
8 device in the embodiment.

9 Figs. 16A and 16B are views showing aspects of the  
10 sector data and the flag bits in another case when data  
11 reading and writing is executed in the state of turning on  
12 the encryption function of the hard disk device in the  
13 embodiment.

14 Fig. 17 is a view showing aspects of the sector data  
15 and the flag bits when data reading and writing is executed  
16 in the state where the encryption function of the hard disk  
17 device is once turned on and then turned off again.

18 Fig. 18 is a view showing a schematic configuration of  
19 a computer device including the hard disk device having the  
20 encryption function according to the present invention.

## 21 DETAILED DESCRIPTION OF THE INVENTION

22 The present invention provides methods, systems and  
23 apparatus to achieve encryption processing of a stored data  
24 and management of an encryption key, which are suitable for  
25 the case when user verification and encryption of the stored  
26 data are applied to a storage device at the same time.

27 The present invention also provides a method of  
28 encryption processing for the stored data suitable for a



1 detachably implemented storage device, and to provide a  
2 storage device which can achieve the method of encryption  
3 processing.

4 In an example embodiment, the present invention will  
5 be realized as a data storage device to be configured as  
6 follows. Specifically, the data storage device includes an  
7 encryption circuit for encrypting desired data and personal  
8 identification information by use of an encryption key  
9 created out of a given piece of the personal identification  
10 information such as a password; a recording medium for  
11 recording the data and the personal identification informa-  
12 tion which are encrypted by the encryption circuit, and a  
13 control unit for executing user verification by use of the  
14 encrypted personal identification information stored in the  
15 recording medium.

16 The encryption key may be further encrypted by use of  
17 another encryption key (a master key) and recorded in the  
18 recording medium. Alternatively, the encryption key may be  
19 recorded without encryption in a special storage area  
20 provided in the recording medium which is not accessible by  
21 normal use. In this way, even if the personal identifica-  
22 tion information is lost (such as the case when a user  
23 forgets a password), it is possible to decrypt and read the  
24 encrypted data by use of the encryption key saved in the  
25 recording medium.

26 Moreover, it is also possible to create a plurality of  
27 encryption keys out of a plurality of personal identifica-  
28 tion information, and to control the user verification and  
29 the data encryption depending on each of the plurality of  
30 encryption keys. In this case, the storage areas are  
31 managed in accordance with the plurality of keys and the

1 encrypted data are recorded in the respective storage areas  
2 by use of the corresponding encryption keys. In this way,  
3 it is possible to verify respective users individually and  
4 to execute the encryption processing by use of the individ-  
5 ual encryption keys when the data storage device is shared  
6 by the plurality of users.

7 Another data storage device according to the present  
8 invention encrypts desired data with an encryption circuit  
9 by use of a first encryption key, and encrypts the first  
10 encryption key and personal identification information by  
11 use of a second encryption key created out of a given piece  
12 of the personal identification information. Then, the data  
13 storage device records the data encrypted by use of the  
14 first encryption key, the first encryption key encrypted by  
15 use of the second encryption key, and the personal identifi-  
16 cation information encrypted by use of the second key in a  
17 recording medium. Moreover, the control unit executes user  
18 verification by use of the encrypted personal identification  
19 information stored in the recording medium. Here, the first  
20 encryption key may be created out of the personal identifi-  
21 cation information as similar to the second key, or alterna-  
22 tively, arbitrary information such as a random number  
23 sequence may be set up and used as the first encryption key.  
24 In such a configuration, the encryption circuit decrypts the  
25 encrypted first encryption key being read out of the record-  
26 ing medium by use of the second encryption key, and thereby  
27 encrypts or decrypts the desired data by use of the  
28 decrypted first encryption key.

29 As described above, although the higher encryption key  
30 is changed if the encryption keys are multiple-layered and  
31 the higher encryption key is created out of the personal

1 identification information so as to change the personal  
2 identification information for enhancing security, it is not  
3 necessary to change the lower encryption key which is  
4 encrypted by use of the higher encryption key. That is, it  
5 is possible to deal with the change of the personal identi-  
6 fication information just by encrypting the lower encryption  
7 key again with the changed higher encryption key, and it is  
8 not necessary to encrypt the data again which are encrypted  
9 by the lower encryption key.

10         Meanwhile, the present invention is also realized as a  
11 data storage device to be configured as follows.  
12 Specifically, the data storage device includes a magnetic  
13 disk, a read-and-write mechanism for reading and writing  
14 data, and a control mechanism which has an encryption  
15 function for encrypting data to be written in the magnetic  
16 disk and for decrypting the encrypted data to be read out of  
17 the magnetic disk, and controls reading and writing of the  
18 data by the reading-and-writing mechanism. Moreover, upon  
19 processing of writing the data in the magnetic disk, the  
20 control mechanism executes encryption of the data to be  
21 written in the magnetic disk for each unit of writing and  
22 reading data in and out of a storage area of the magnetic  
23 disk in response to turning on and off of the encryption  
24 mechanism. Here, the unit of data writing and reading in  
25 and out of the storage area of the magnetic disk may be  
26 defined as equivalent to a sector, a logical block, or the  
27 like. Moreover, upon reading the data out of the storage  
28 medium, the control mechanism judges as to whether the data  
29 are encrypted or not, and further controls decryption when  
30 the data are encrypted.

31         Meanwhile, another way of attaining the foregoing

1 aspects is also realized as a data processing method for  
2 executing data writing and reading in and out of a recording  
3 medium of a data storage device, which is configured as  
4 follows. Specifically, the data processing method includes  
5 the steps of creating an encryption key by converting a  
6 given piece of personal identification information with an  
7 encryption function or a one-way function, encrypting the  
8 personal identification information by use of the created  
9 encryption key and thereby recording the encrypted personal  
10 identification information in a recording medium as verifi-  
11 cation data, executing user verification based on the  
12 verification data, and encrypting write data transmitted  
13 from a host system by use of the previously created encryp-  
14 tion key and thereby recording the encrypted write data in  
15 the recording medium or decrypting the data read out of the  
16 recording medium by use of the encryption key and thereby  
17 transmitting the decrypted data to the host system.

18 Moreover, another data processing method according to  
19 the present invention includes the steps of creating an  
20 verification encryption key out of a given piece of personal  
21 identification information, encrypting the personal identi-  
22 fication information by use of the verification encryption  
23 key and thereby recording the encrypted personal identifica-  
24 tion information in a recording medium as verification data  
25 while encrypting a data encryption key by use of the verifi-  
26 cation encryption key and thereby recording the encrypted  
27 data encryption key in the recording medium, executing user  
28 verification based on the verification data, decrypting the  
29 data encryption key by use of the verification encryption  
30 key, and encrypting write data transmitted from a host  
31 system by use of the decrypted data encryption key and

1     thereby recording the encrypted write data in the recording  
2     medium or decrypting the data read out of the recording  
3     medium by use of the data encryption key and thereby trans-  
4     mitting the decrypted data to the host system.

5             Moreover, the present invention is also realized as a  
6     program which controls a computer to execute processing  
7     which corresponds to the respective steps of any of the  
8     above-described data processing methods.

9             Furthermore, the present invention can be also  
10    realized as an information processing device which incorpo-  
11    rates and use any of the above-described data storage  
12    devices as an external storage device.

13            Now, the present invention will be described in detail  
14    based on embodiments as illustrated in the accompanying  
15    drawings. Although the present invention refers to encryp-  
16    tion technology which is applicable to various types of  
17    external storage devices including magnetic disk devices  
18    (such as hard disk devices), optical disk devices, memory  
19    cards and the like, description will be made in this embodi-  
20    ment regarding application to a hard disk device as an  
21    example.

22            A hard disk device is used as an external storage  
23    device for a personal computer, a workstation, or any other  
24    computer device (an information processing device).

25            Fig. 18 is a view showing a schematic configuration of  
26    a computer device including the hard disk device as the  
27    external storage device.

28            As shown in Fig. 18, a computer device 200 includes an  
29    operation control unit 210 realized by a central processing  
30    unit (CPU) and an internal memory such as a random access  
31    memory (RAM), and an interface 220 (such as an AT attachment

1 (ATA) or a small computer system interface (SCSI)) for  
2 accessing a hard disk device 100 which is an external  
3 storage device. The computer incorporates the hard disk  
4 device 100 as the external storage device. The hard disk  
5 device 100 stores (writes) and transfers (reads) data in  
6 accordance with control by the operation control unit 210 of  
7 the computer device 200. Here, although illustration is not  
8 specifically made in the drawing, it is obvious that the  
9 computer device 200 is actually configured by including  
10 inputting means such as a keyboard or a mouse for inputting  
11 the data or commands, and outputting means such as a display  
12 device for outputting processing results, and the like.

13 Fig. 1 is a view showing a configuration example of  
14 the hard disk device 100 of this embodiment.

15 With reference to Fig. 1, the hard disk device 100  
16 includes a magnetic disk 10, which is a recording medium.  
17 Moreover, the hard disk device 100 also includes a  
18 read/write head 20, a spindle motor for rotating the  
19 magnetic disk 10 and a voice coil motor for seeking the  
20 read/write head 20 (which are collectively denoted as the  
21 motors 30 in the drawing), and a read/write channel 40 for  
22 executing data reading and writing processing by modulating  
23 and demodulating data (signals) for writing and reading in  
24 and out of the magnetic disk 10 through the read/write head  
25 20, collectively as a read-and-write mechanism for data  
26 writing and reading in and out of the magnetic disk 10.  
27 Furthermore, the hard disk 100 also includes a hard disk  
28 controller 50 for supervising and controlling operations of  
29 the hard disk device 100, and a buffer memory 60, collec-  
30 tively as a control mechanism.

31 The hard disk controller 50 includes a drive interface

1 51 for exchanging data with the read/write channel 40, an  
2 error correction circuit 52 for correcting a reading error  
3 in the data read out of the magnetic disk 10, a memory  
4 control circuit 53 for accessing the buffer memory 60, an  
5 encryption circuit 54 and a selector 55 for encrypting and  
6 decrypting the data to be read out of and written into the  
7 magnetic disk 10, an I/O interface 56 for exchanging the  
8 data and commands with the computer device 200 being the  
9 host system, a servo control circuit 57 for performing servo  
10 control based on servo signals read out of the magnetic disk  
11 10 with the read/write head 20, and a CPU 58 as a control  
12 unit for performing operation control of the respective  
13 circuits.

14 In the above-described configuration, when data are  
15 written in the magnetic disk 10, a write request command  
16 transmitted from the computer device 200 is firstly received  
17 by the CPU 58 through the I/O interface 56, and then the  
18 following operations are conducted under the control by the  
19 CPU 58. Specifically, write data transmitted from the  
20 computer device 200 after the write request command are  
21 inputted through the I/O interface 56 and are encrypted by  
22 the selector 55 and the encryption circuit 54 as  
23 appropriate, and then are transmitted from the drive inter-  
24 face 51 to the read/write channel 40 through buffering by  
25 the memory control circuit 53 and the buffer memory 60.  
26 Thereafter, the data are magnetically written in the  
27 magnetic disk 10 with the read/write head 20. Here, physi-  
28 cal operations such as seeking with the read/write head 20  
29 or rotation of the magnetic disk 10 are controlled by CPU 58  
30 through the servo control circuit 57 and the motors 30.  
31 Details of the control for the encryption processing by the

1 selector 55 and the encryption circuit 54 will be described  
2 later.

3         Meanwhile, when the data are read out of the magnetic  
4 disk 10, a read request command transmitted from the  
5 computer device 200 is firstly received by the CPU 58  
6 through the I/O interface 56, and then the following opera-  
7 tions are executed under the control by the CPU 58.  
8 Specifically, operations of the read/write head 20 and the  
9 magnetic disk 10 are controlled by the servo control circuit  
10 57 and the motors 30, and thereby the data recorded in a  
11 desired area of the magnetic disk 10 are read out. The data  
12 thus read out are transmitted to the hard disk controller 50  
13 through the read/write channel 40, and are further transmit-  
14 ted to the error correction circuit 52 through the drive  
15 interface 51. After errors such as garbled bits are  
16 corrected by the error correction circuit 52, the data are  
17 decrypted by the selector 55 and the encryption circuit 54  
18 as appropriate and then transmitted to the computer device  
19 200 through the I/O interface 56. Details of the control  
20 for the decryption processing by the selector 55 and the  
21 encryption circuit 54 will be described later.

22         In this embodiment, encryption of the data to be  
23 written in the magnetic disk 10 and decryption of the data  
24 to be read out of the magnetic disk 10 are controlled by use  
25 of the encryption circuit 54 and the selector 55 which are  
26 under control of the CPU 58.

27         The encryption circuit 54 encrypts the data and  
28 decrypts the encrypted data by use of an encryption  
29 algorithm. The selector 55 selects as to whether or not the  
30 write data or the read data are subjected to processing by  
31 the encryption circuit 54.



1           The processing by the encryption function of this  
2   embodiment is divided broadly into two categories of: (A)  
3   processing concerning management of an encryption key when  
4   user verification and encryption of the stored data are  
5   applied at the same time; and (B) processing concerning  
6   control for encryption and decryption of the stored data to  
7   be written in the magnetic disk 10. Description will be  
8   made below regarding each of the categories.

9   A. Processing concerning management of an encryption key

10           In this processing, the same encryption algorithm is  
11   used for the user verification and the encryption processing  
12   of the stored data. Specifically, the encryption key for  
13   use in encryption and decryption of the stored data is  
14   created by converting the personal identification informa-  
15   tion used for the user verification with an encryption  
16   function or a one-way function. Then, the encryption  
17   circuit 54 further encrypts the personal identification  
18   information by use of this encryption key, and the encrypted  
19   personal identification information (hereinafter referred to  
20   as the "verification data") are written and saved in the  
21   magnetic disk 10. Upon the user verification, the CPU 58  
22   firstly requests input of the personal identification infor-  
23   mation, then converts the personal identification informa-  
24   tion inputted to the encryption circuit 54 with the same  
25   encryption algorithm. Thereafter, the CPU 58 judges as to  
26   whether or not the converted data match the verification  
27   data written in the magnetic disk 10, and identifies the  
28   qualified user based on a result of the judgment. Even if  
29   the verification data written in the magnetic disk 10 are  
30   illegally read out, the original personal identification  
31   information will not be obtained because of the one-way

1 property of the encryption processing (that the original  
2 data cannot be obtained without the encryption key).

3 Here, in addition to a password in a password lock  
4 function to be included in the hard disk device 100 as a  
5 standard equipment, a variety of information can be used as  
6 the personal identification information, such as a character  
7 string of an arbitrary length, ID information recorded in an  
8 IC card or the like, or biological information according to  
9 biometrics by use of fingerprints and the like.

10 Now, the respective operations of the method of the  
11 present invention will be separately described.

12 1. Initial setting (creation of the encryption key and  
13 saving the verification data)

14 Fig. 2 is a view describing the method of initial  
15 setting of the user verification.

16 As shown in Fig. 2, the encryption key is firstly  
17 created by encrypting the personal identification informa-  
18 tion with the encryption circuit 54 (1-a). When the data  
19 length of the personal identification information is too  
20 short, such a shortage can be padded with appropriate data.  
21 On the contrary, when the data length of the personal  
22 identification information is too long, the encryption can  
23 be compressed to a desired key length by use of common key  
24 encryption in a message verification code (MAC) mode, which  
25 is a feedback mode. Moreover, as for the encryption key to  
26 be used in such encryption, it is possible to use a part of  
27 the personal identification information or appropriate key  
28 information (data) may be set up instead.

29 Next, the personal identification information is  
30 encrypted again and thereby converted into the verification  
31 data with the encryption circuit 54 by use of the encryption

1 key created in the processing (1-a), and then the verifica-  
2 tion data are written in the magnetic disk 10 (1-b). It is  
3 also possible to divide the personal identification informa-  
4 tion in two pieces and each piece may be provided for  
5 creation of the encryption key and for creation of the  
6 verification data, as long as input of the personal identi-  
7 fication information of a sufficient data length is ensured.

8 From that time on, the encryption key created in the  
9 processing (1-a), which is used for creation of the verifi-  
10 cation data, will be used for encryption and decryption of  
11 the data to be written in and read out of the magnetic disk  
12 10 by the encryption circuit 54 (1-c).

13 2. The user verification and the encryption processing of  
14 the stored data

15 Fig. 3 is a view describing a method of the user  
16 verification and the encryption processing of the stored  
17 data.

18 As shown in Fig. 3, the personal identification infor-  
19 mation is firstly inputted and then encrypted by the encryp-  
20 tion circuit 54, whereby the encryption key is created  
21 (2-a). Then, the personal identification information is  
22 encrypted again with the encryption circuit 54 by use of  
23 this encryption key, and the verification data are created  
24 (2-b). When the inputted personal identification informa-  
25 tion is correct (in other words, when the inputted personal  
26 identification is identical to the personal identification  
27 information which was used upon creation of the encryption  
28 key and the verification data in the initial setting  
29 described with reference to Fig. 2), the created verifica-  
30 tion data match the verification data that are recorded in  
31 the magnetic disk 10. Accordingly, the verification

1 succeeds in the verification processing by the CPU 58 and  
2 the hard disk device 100 is thereby activated. Then, either  
3 encryption of the data to be transmitted from the computer  
4 device 200 and to be written in the magnetic disk 10, or  
5 decryption of the data read out of the magnetic disk 10 and  
6 to be transmitted to the computer device 200 is executed by  
7 the encryption circuit 54 (2-c).

8 On the contrary, when the inputted personal identifi-  
9 cation information is wrong (in other words, when the input-  
10 ted personal identification is not identical to the personal  
11 identification information which was used upon creation of  
12 the encryption key and the verification data in the initial  
13 setting described with reference to Fig. 2), the created  
14 verification data do not match the verification data that  
15 are recorded in the magnetic disk 10. Accordingly, the  
16 verification fails and the hard disk device 100 is thereby  
17 locked (to an inaccessible state) (2-a') (2-b'). Therefore,  
18 data reading or writing in and out of the magnetic disk 10  
19 are unable. Even if the encrypted stored data in the  
20 magnetic disk 10 are read out somehow or other, the data  
21 cannot be decrypted because the correct encryption key is  
22 not created (2-c'). In addition, it is not possible to  
23 restore the encryption key or the personal identification  
24 information out of the encrypted verification data stored in  
25 the magnetic disk 10 because of the one-way property of the  
26 encryption processing.

### 27 3. Recovery of the stored data

28 Fig. 4 is a view describing a method to recover the  
29 stored data when a trouble occurs in the magnetic disk 10.

30 When a trouble occurs in the magnetic disk 10, if it  
31 is possible to read the stored data at least partially (3-a)

1 as shown in Fig. 4, an encryption key is created out of the  
2 personal identification information by use of encryption  
3 software or the like (3-b) based on an algorithm as similar  
4 to the encryption processing by the encryption circuit 54,  
5 so that the data in the read-out portion can be restored  
6 (3-c).

7 In this embodiment, safety of the encrypted stored  
8 data will not be damaged even if the algorithms for the  
9 verification and the encryption are disclosed. This is  
10 because the encrypted data are protected by the encryption  
11 key which is created out of the personal identification  
12 information of the respective users. In other words, it is  
13 impossible to decrypt the encrypted data unless the encryp-  
14 tion key created out of the personal identification informa-  
15 tion in accordance with the above-described procedures (see  
16 the operations 1 and 2) is used. Accordingly, it is not  
17 possible to recover the personal identification information  
18 or the original data out of the verification data or the  
19 encrypted data. Therefore, in the case of a breakdown of  
20 the hard disk device 100 or the like, there is no concern  
21 that a third party obtains the contents of the stored data  
22 even if the user asks the third party to cancel the lock for  
23 the user verification and to read the data.

24 Here, when a trouble occurs in a mechanical portion  
25 other than the magnetic disk 10, such as in a circuit on a  
26 board, it is possible to recover from such a trouble without  
27 reading the data for restoration as described above, but  
28 just with setting the relevant magnetic disk 10 onto another  
29 hard disk device 100.

#### 30 4. Recovery of the stored data using a master key

31 Fig. 5 is a view describing a method to recover the

1 stored data by use of a master key.

2 As shown in Fig. 5, the personal identification infor-  
3 mation is firstly encrypted by the encryption circuit 54,  
4 and the encryption key is thereby created (4-a). Then, this  
5 encryption key is encrypted by use of a separately created  
6 master key (4-b), and is written and saved in the magnetic  
7 disk (4-c). The stored data are encrypted or decrypted  
8 (4-d) by use of the encryption key, which is created in the  
9 processing (4-a).

10 When the encrypted encryption key is saved in the  
11 magnetic disk 10 as described above, the encryption key can  
12 be restored by use of the master key (4-e) even if the use  
13 loses the personal identification information (such as the  
14 case when the user forgets the password). Accordingly, it  
15 is possible to read and decrypt the encrypted stored data  
16 (4-f).

17 It is conceivable that this master key is created and  
18 preserved by the manufacturer of the hard disk device 100  
19 for use in repair and maintenance of the product. Note that  
20 security of the stored data is relatively decreased in this  
21 case, because the owner of the master key is able to access  
22 the stored data which are encrypted by the user. Meanwhile,  
23 if the hard disk device 100 is completely locked by the  
24 personal identification information, there is no chance to  
25 read the encrypted data upon a failure and the like of the  
26 hard disk device 100. Accordingly, it is also important to  
27 provide various security level options to be flexibly set in  
28 response to the request of the user, such as an option not  
29 to allow the lock by the user verification upon encryption  
30 of the stored data or an option to allow the master key  
31 solely to release the lock by the user verification.

1     5. Multiple setting of the verification data

2             Upon a failure of the hard disk device 100, it is  
3     necessary to cancel the lock function of the hard disk  
4     device 100 for a failure analysis irrespective of the recov-  
5     ery of the stored data. Therefore, it is convenient if  
6     separate verification data for canceling the lock of the  
7     hard disk device 100 in addition to the verification data  
8     used for locking the hard disk device 100 and for the  
9     encryption of the stored data (the verification data created  
10    out of the personal identification data).

11            Fig. 6 is a view describing a method of setting the  
12    verification data for canceling the lock of the hard disk  
13    device 100 in addition to the verification data according to  
14    the personal identification information.

15            As shown in Fig. 6, in addition to the processes in  
16    the operation 1 where the encryption key is created out of  
17    the personal identification information (5-a) and the  
18    verification data are created (5-b), verification informa-  
19    tion different from the personal identification information  
20    is encrypted by the encryption circuit 54 and is written and  
21    saved in the magnetic disk 10 as other verification data  
22    (5-c). The user verification using the verification data is  
23    executed by the CPU 58 as similar to the operation 2.

24            Since the verification data are not related to the  
25    encryption key, the verification data cannot recover the  
26    stored data unlike the master key described in the operation  
27    4. Therefore, there is no risk of leakage of the contents  
28    in the stored data even if a third party possesses the  
29    verification information. In addition, it is also useful to  
30    prepare a plurality of pieces of the verification data and  
31    the encryption keys in order to share the hard disk device

1 100 with a plurality of users or to allow the manufacturer  
2 of the hard disk device 100 to secure an exclusive data area  
3 for the system on the magnetic disk 10. In this case, the  
4 storage area of the magnetic disk 10 is managed depending on  
5 the respective pieces of the verification data or the  
6 respective encryption keys, or the storage area of the  
7 magnetic disk 10 is physically divided (into partitions, for  
8 example), whereby the user verification and the encryption  
9 processing are individually controlled. In other words, the  
10 data encrypted by the encryption key are written in the  
11 corresponding storage area out of the storage areas which  
12 are managed depending on the verification data and the  
13 encryption keys.

14 6. Support to a change in the personal identification  
15 information

16 Fig. 7 and Fig. 8 are views describing a method for  
17 the encryption processing in a case of changing the personal  
18 identification information.

19 Upon the user verification, it is suggested to change  
20 the personal identification information for verification  
21 periodically or at random to enhance the security. However,  
22 when the stored data are simply encrypted by use of the  
23 encryption key which is created out of the personal identi-  
24 fication information, the encryption will be changed if the  
25 personal identification information is changed.

26 Accordingly, it is necessary to execute the processing of  
27 decrypting the stored data with the encryption key created  
28 out of the personal identification information prior to the  
29 change and then encrypting the stored data again with an  
30 encryption key created out of the new personal information.  
31 The storage capacity of the hard disk device 100 is



1 increasing these days, and there may be a case where data  
2 exceeding 100 GB are stored therein. Accordingly, it will  
3 take a lot of time for decryption and re-encryption of such  
4 huge data. Therefore, a data encryption key used for the  
5 encryption processing of the stored data is encrypted and  
6 saved by use of the verification encryption key which is  
7 created by encrypting the personal identification informa-  
8 tion. In this way, it is possible to the change in the  
9 personal identification information without degrading the  
10 security. Here, the encryption key described in the opera-  
11 tions 1, 2 and the like is deemed to be the case where the  
12 data encryption key and the verification encryption key  
13 described herein are identical to each other (not that the  
14 encryption key is not saved in the magnetic disk 10 at the  
15 initial setting of the operation 1).

16 An operation at the initial setting will be described  
17 with reference to Fig. 7.

18 As shown in Fig. 7, the personal identification infor-  
19 mation is firstly encrypted by the encryption circuit 54,  
20 whereby the verification encryption key is created (6-a).  
21 Then, the personal identification information is encrypted  
22 again by use of this verification encryption key, and the  
23 encrypted personal identification information is written and  
24 saved in the magnetic disk 10 as the verification data  
25 (6-b). Similarly, the data encryption key is encrypted by  
26 use of this verification encryption key, and the encrypted  
27 data encryption key is written and saved in the magnetic  
28 disk 10 (6-c). In this operation 6, the data encryption key  
29 exclusive for the data encryption processing is used for  
30 encryption of the read data and decryption of the write data  
31 (6-d), instead of the verification encryption key created

1 out of the personal identification information in the  
2 processing (6-a). As similar to the verification encryption  
3 key and the above-described operations 1, 2 and the like,  
4 this data encryption key may be created by encrypting given  
5 information for creation of the encryption key with the  
6 encryption circuit 54, or arbitrary key information (such as  
7 a random number sequence) may be set up and used as the  
8 encryption key. Moreover, it is also possible to create the  
9 data encryption key by encrypting the same personal identi-  
10 fication information as the verification encryption key by  
11 use of an encryption function or a one-way function which is  
12 different from one used upon creation of the verification  
13 encryption key. Here, when the mutually different verifica-  
14 tion encryption key and the data encryption key are created  
15 out of the personal identification information by use of  
16 different operations (functions), it is possible to create  
17 the correct data encryption key if the personal identifica-  
18 tion information is correct. Accordingly, it is not neces-  
19 sary to encrypt the data encryption key with the  
20 verification encryption key and to save the data encryption  
21 key in the magnetic disk 10.

22 Next, description will be made regarding the user  
23 verification and the encryption processing of the stored  
24 data with reference to Fig. 8.

25 As shown in Fig. 8, the personal identification infor-  
26 mation is firstly encrypted by the encryption circuit 54,  
27 whereby the verification encryption key is created (2-e).  
28 Then, the personal identification information is encrypted  
29 again by use of this verification encryption key, and the  
30 verification data are created (6-f). When the created  
31 verification data are identical to the verification data

1 recorded in the magnetic disk 10, the verification succeeds  
2 in the verification processing by the CPU 58 and the hard  
3 disk device 100 is thereby activated (6-g). Moreover, the  
4 encrypted data encryption key is read out of the magnetic  
5 disk 10 and is decrypted with the encryption circuit 54 by  
6 use of the verification encryption key (6-h). Then, either  
7 encryption of the data to be transmitted from the computer  
8 device 200 and to be written in the magnetic disk 10, or  
9 decryption of the data read out of the magnetic disk 10 and  
10 to be transmitted to the computer device 200 is executed by  
11 the encryption circuit 54 using the data encryption key  
12 (6-i).

13 When the encryption processing for the stored data is  
14 performed as shown in Fig. 7 and Fig. 8, even if the  
15 personal identification information is changed, it is only  
16 necessary to create verification data again out of new  
17 personal identification information and to encrypt a data  
18 encryption key again with a new verification encryption key  
19 to be created out of the new personal identification infor-  
20 mation. In other words, it is not necessary to encrypt the  
21 entire stored data again. Therefore, it is possible to  
22 respond with realistic processing if a large amount of the  
23 stored data are recorded in the magnetic disk 10.

24 Fig. 9 is a view describing an operation of changing  
25 the personal identification information.

26 As shown in Fig. 9, the verification encryption key is  
27 firstly created out of the personal identification informa-  
28 tion before the change by the encryption circuit 54 (6-j),  
29 and the verification data are created out of the personal  
30 identification information by use of this verification  
31 encryption key. Then, the created verification data are

1 verified with the verification data recorded in the magnetic  
2 disk 10 by the CPU 58 (6-k). After the verification is  
3 completed, the encrypted data encryption key recorded in the  
4 magnetic disk 10 is read out and decrypted with the encryp-  
5 tion circuit 54 by use of the verification encryption key  
6 (6-l).

7 Meanwhile, the new verification encryption key is  
8 created out of the new personal identification information  
9 (6-m), and the personal identification information is  
10 encrypted again by use of the new verification encryption  
11 key, whereby the encrypted personal identification informa-  
12 tion is written and saved in the magnetic disk 10 as the new  
13 verification data (6-n). Thereafter, the data encryption  
14 key being decrypted previously is encrypted again with the  
15 encryption circuit 54 by use of the new verification encryp-  
16 tion key, and the encrypted data encryption key is written  
17 and saved in the magnetic disk 10 (6-o).

18 Moreover, when the encryption processing for the  
19 stored data is performed as shown in Fig. 7 and Fig. 8, even  
20 if the hard disk device 100 is failed, it is still possible  
21 to decrypt the stored data with the data encryption key and  
22 thereby obtain the desired data as long as the encrypted  
23 stored data can be read out of the magnetic disk 10, either  
24 by obtaining the data encryption key as similar to the  
25 encryption of the stored data, or by creating the verifica-  
26 tion encryption key out of the personal identification  
27 information and then restoring the data encryption key.

28 Figs. 10A and 10B are views describing a method of  
29 data recovery.

30 If the data encryption key is created by encrypting  
31 the information for creation of the encryption key with the

1 encryption circuit 54, as shown in Fig. 10A, it is possible  
2 to create the data encryption key again by encrypting the  
3 same information by use of the same encryption logic as that  
4 of the encryption circuit 54 (6-p). Then, the stored data  
5 read out of the magnetic disk 10 are decrypted by use of  
6 this data encryption key (6-q).

7 Meanwhile, the verification encryption key is created  
8 by encrypting the personal identification information by use  
9 of the same encryption logic as that of the encryption  
10 circuit 54 (6-r). Therefore, if the encrypted data encryp-  
11 tion key can be read out of the magnetic disk 10, as shown  
12 in Fig. 10B, the data encryption key is decrypted by use of  
13 this verification encryption key (6-s). Thereafter, the  
14 stored data read out of the magnetic disk 10 are decrypted  
15 by use of this data encryption key (6-t).

#### 16 7. Cancel of the user verification

17 A command to clear the password is set as standard  
18 equipment on the hard disk device 100 having the password  
19 lock function. After execution of this command, it is  
20 essential that anybody can read and write the contents in  
21 the disk. However, if the stored data in the magnetic disk  
22 10 are encrypted, the entire decryption of the encrypted  
23 stored data and rewriting of the decrypted data in the  
24 magnetic disk 10 along with the cancel of the user verifica-  
25 tion require a lot of time and are therefore impractical.  
26 Therefore, when the user verification is canceled, the  
27 encryption key to be used for the encryption processing of  
28 the stored data is written in the magnetic disk 10, so that  
29 the encryption key can be used by anybody at any time  
30 (without the verification) upon reading the stored data.

31 When the encryption processing for the stored data is

1 performed as shown in Fig. 7 and Fig. 8, the encrypted data  
2 encryption key is saved in the magnetic disk 10. Therefore,  
3 anybody can freely use the data encryption key by decrypting  
4 the data encryption key and writing the data encryption key  
5 in the magnetic disk 10.

6 Fig. 11 is a view describing a method of setting the  
7 data encryption key to be usable by anybody along with the  
8 cancel of the user verification.

9 As shown in Fig. 11, the verification encryption key  
10 is firstly created out of the personal identification infor-  
11 mation before the change by the encryption circuit 54 (7-a),  
12 and the verification data are created out of the personal  
13 identification information by use of this verification  
14 encryption key. Then, the created verification data are  
15 verified with the recorded verification data recorded in the  
16 magnetic disk 10 by the CPU 58 (7-b). After the verifica-  
17 tion is completed, the encrypted data encryption key  
18 recorded in the magnetic disk 10 is read out and decrypted  
19 with the encryption circuit 54 by use of the verification  
20 encryption key (7-c). Then, the decrypted data encryption  
21 key is written in the magnetic disk 10 again (7-d). There-  
22 after, the data encryption upon data reading and writing  
23 becomes possible by use of the data encryption key written  
24 in the magnetic disk 10 (7-e).

25 After the encryption key (the data encryption key) is  
26 rendered freely usable by anybody as described above, if the  
27 encryption in the event of writing the data in the magnetic  
28 disk 10 and the decryption in the event of reading the data  
29 out of the magnetic disk 10 are automatically performed  
30 under the control by the CPU 58, the user can read and write  
31 the data in and out of the magnetic disk 10 without

1 recognition that the stored data are encrypted. Moreover,  
2 it is also possible to control not to encrypt the data which  
3 will be written in the magnetic disk 10 after the user  
4 verification is canceled. In this case, in order to judge  
5 as to whether the processing by the encryption circuit 54 is  
6 executed or not upon reading or writing the stored data in  
7 accordance with encryption or unencryption of the stored  
8 data, it is necessary to distinguish the encrypted stored  
9 data and the unencrypted stored data by means of adding flag  
10 bits or the like.

11 When the user verification is canceled as described  
12 above, the unencrypted encryption key (the data encryption  
13 key) is temporarily recorded in the magnetic disk 10 during  
14 a series of processing of "setting the user verification" -  
15 "canceling the user verification" - "setting the user  
16 verification". Therefore, if the encryption key is read out  
17 by a third party in this event, the third party may be able  
18 to decrypt the stored data in the magnetic disk 10 by use of  
19 the encryption key. However, since a special storage area  
20 which is not normally accessible by the user is provided on  
21 the magnetic disk 10 in the usual hard disk device 100.  
22 Accordingly, upon recording the unencrypted encryption key,  
23 it is possible to avoid the encryption key from being easily  
24 read out by the third party if the special storage area is  
25 used.

26 Nevertheless, it is still possible to read the data  
27 written in the relevant storage area by use of a special  
28 measuring device. Accordingly, there remains a risk that  
29 the stored data would be decrypted by the third party if the  
30 hard disk device 100 itself falls into the hand of the third  
31 party.

1           The following case is conceivable as a concrete  
2 example.

3           Here, an assumption is made that a malicious third  
4 party passes a hard disk device 100 to a target user who  
5 intends to steal data for, and that the third party acquired  
6 an unencrypted encryption key (a data encryption key) for  
7 the hard disk device 100 beforehand by the procedures of  
8 "setting the user verification" - "canceling the user  
9 verification" - "setting the user verification". In this  
10 case, the data stored in the hard disk device 100 by the  
11 target user can be decrypted by use of the encryption key  
12 acquired by the malicious third party even if the data are  
13 encrypted.

14           However, it is easy to check as to whether or not  
15 cancel or setting of user verification has been executed on  
16 the hard disk device 100 after shipment. Accordingly, if a  
17 risk of such data theft becomes apparent as a result of the  
18 check, it is possible to cope with the risk by formatting a  
19 magnetic disk 10 again or by re-encrypting the encrypted  
20 data with a new encryption key, although such measures are  
21 somewhat time-consuming.

#### 22 8. Recovery of the stored data using a master key

23           Instead of encrypting the data encryption key by use  
24 of the verification encryption key as described in the  
25 operation 6, it is also possible to encrypt the data encryp-  
26 tion key by use of a master key and to save the encrypted  
27 data encryption key in the magnetic disk 10.

28           Fig. 12 is a view describing a method to recover the  
29 stored data by use of the master key.

30           As shown in Fig. 12, the personal identification  
31 information is firstly encrypted by the encryption circuit



1 54, whereby the verification encryption key is created  
2 (8-a). Then, the verification data are created by encrypt-  
3 ing the personal identification information again with the  
4 encryption circuit 54 by use of this verification encryption  
5 key, and the verification data are written and saved in the  
6 magnetic disk 10 (8-b). Meanwhile, the data encryption key  
7 is encrypted by use of a separately created master key, and  
8 the encrypted data encryption key is written and saved in  
9 the magnetic disk 10 (8-c). The data encryption key is used  
10 for encryption and decryption of the stored data (8-d). As  
11 similar to the operation 6, the data encryption key may be  
12 created by encrypting given information for creation of the  
13 encryption key with the encryption circuit 54, by setting  
14 arbitrary key information such as a random number sequence,  
15 or by encrypting the personal identification information  
16 with a function which is different from the one used upon  
17 creation of the verification encryption key.

18 If the encrypted data encryption key created as  
19 described above is saved in the magnetic disk 10, the data  
20 encryption key can be restored by use of the master key  
21 (8-e). Accordingly, an owner of the master key can read and  
22 decrypt the encrypted stored data freely (8-f) even if the  
23 user does not decrypt the data encryption key or save the  
24 decrypted encryption key in the magnetic disk 10 as  
25 described in the operation 7.

26 B. Processing concerning control for encryption and decryp-  
27 tion of the stored data

28 In this processing, encryption processing on data is  
29 controlled for each unit of writing and reading the data in  
30 and out of the recording medium in response to turning on  
31 and off of the encryption function of the hard disk device

1 100. The unit of reading and writing the data may be  
2 defined as a sector or a logical block to be set in the  
3 storage area of the magnetic disk 10, for example. In the  
4 following, description will be made regarding the case where  
5 the encryption is controlled depending on sectors. Here,  
6 switching work for turning the encryption function on and  
7 off in the hard disk device 100 can be executed, for  
8 example, by means of issuing a switching command from the  
9 computer device, the host system, through a hard disk driver  
10 or the like. Meanwhile, it is also possible to switch the  
11 encryption function on and off by use of a physical switch  
12 (such as a jumper switch) provided on a hard ware casing.

13 The processing unit in a common key encryption method  
14 which is widely used for data encryption is normally either  
15 a 64-bit or 128-bit basis. In this case, a disk sector in  
16 the size of 512 bytes (4096 bits) will be divided into 64 or  
17 32 blocks for the encryption processing. Typical use modes  
18 of the encryption include the electronic code book (ECB)  
19 mode and the cipher block chaining (CBC) mode.

20 Fig. 13 is a view showing the concepts of the encryption  
21 and decryption processing in the ECB mode and the CBC mode.

22 As shown in Fig. 13, when plaintext (unencrypted data)  
23 blocks  $P_i$  ( $i=0, 1, 2$ , and so on) created by dividing the  
24 sectors are encrypted in the ECB mode, it is impossible to  
25 find the original plaintext block  $P_i$  by calculation out of a  
26 corresponding ciphertext block  $C_i$ . However, since 64-bit or  
27 128-bit ciphertext blocks of the same values correspond to  
28 the plaintext of the same values, information as to which  
29 pieces of data are identical to each other becomes  
30 disclosed.

31 For this reason, the CBC mode is applied to the case

1 of encrypting data having a considerable data length. The  
2 CBC is an encryption mode which applies continuous calcula-  
3 tion of an exclusive OR (XOR) of an object data block and a  
4 previous data block. Upon encryption in the CBC mode as  
5 shown in Fig. 13, the plaintext block  $P_i$  is encrypted after  
6 the XOR operation with the previous encrypted block  $C_{i-1}$ . In  
7 this way, the same plaintext blocks will be converted into  
8 different ciphertext blocks.

9 In the CBC mode, the initial plaintext block  $P_0$  does  
10 not have a ciphertext block targeted for the XOR operation.  
11 In this case, typically, an appropriate data piece called an  
12 initial vector (IV) is encrypted to create a pseudo-random  
13 number  $C_{IV}$ , and then the pseudo-random number  $C_{IV}$  is  
14 subjected to the XOR operation with the plaintext block  $P_0$ .  
15 In this embodiment, a sector number for identifying each  
16 sector will be used as this initial vector. Here, in the  
17 case of the encryption processing of the data by a unit  
18 other than the sector, information for specifying the unit  
19 may be used as the initial vector (for example, a logical  
20 block address (LBA) may be used when a logical block is  
21 defined as the unit of the encryption processing).

22 Fig. 14 is a view schematically showing a data  
23 configuration of the sector corresponding to the encryption  
24 processing of this embodiment.

25 With reference to Fig. 14, each sector records a  
26 sector number 1401 for identifying an individual sector,  
27 sector data 1402 being the stored data, and a flag bit 1403  
28 being a control flag indicating as to whether the sector  
29 data 1402 are encrypted or not.

30 Here, the flag bit 1403 of the sector including the  
31 unencrypted sector data 1402 will be set to "0", and the

1 flag bit 1403 of the sector including the encrypted sector  
2 data 1402 will be set to "1". Therefore, the flag bits 1403  
3 of the respective sectors in the magnetic disk 10 will be  
4 reset to "0" in an initial state, such as a point of  
5 shipment, of the hard disk device 100 because the encryption  
6 function is turned off.

7 In this embodiment, the two following types of control  
8 will be executed upon the encryption processing of the  
9 stored data. Specifically, in the data writing processing,  
10 control is made as to whether or not the data to be written  
11 in the magnetic disk 10 are encrypted in response to turning  
12 on and off of the encryption function in the hard disk  
13 device 100. Meanwhile, in the data reading processing, the  
14 data being read out are decrypted when the stored data are  
15 the encrypted data (when the values of the flag bits 1403  
16 are set to "1").

17 In the hard disk device 100 shown in Fig. 1, the  
18 selector 55 checks turning on and off of the encryption  
19 function and the value of the flag bit 1403 regarding each  
20 piece of the read and write data in each sector, and the  
21 selector 55 can judge as to whether or not encryption of the  
22 write data or decryption of the read data should be executed  
23 by the encryption circuit 54.

24 Fig. 15 is a view showing aspects of the sector data  
25 1402 and the flag bits 1403 when data reading and writing is  
26 executed in the state of turning off the encryption function  
27 of the hard disk device 100.

28 When data reading and writing is executed in the state  
29 where the encryption function of the hard disk device 100 is  
30 kept turned off, the sector data 1402 are unencrypted raw  
31 data and the value of the flag bit 1403 is kept to "0".

1           In the example shown in Fig. 15, the sector data 1402  
2     corresponding to the sector numbers "0" and "2" are read out  
3     and written again. However, those data are not encrypted  
4     and the values of the corresponding flag bits 1403 remain at  
5     "0".

6           Figs. 16A and 16B are views showing aspects of the  
7     sector data 1402 and the flag bits 1403 when data reading  
8     and writing is executed in the state of turning on the  
9     encryption function of the hard disk device 100.

10          When the encryption function of the hard disk device  
11     100 is turned on, encryption will be executed in the data  
12     writing thereafter and the value of the flag bit 1403 will  
13     be set to "1". In other words, after the encryption  
14     function is turned on, the stored data in the magnetic disk  
15     10 will be stepwise encrypted every time the data writing  
16     processing takes place. For this reason, the user can  
17     access the data immediately after turning the encryption  
18     function on without waiting for the entire encryption of the  
19     stored data.

20          In reading the stored data, data are read out directly  
21     if the value of the flag bit 1403 is set to "0" (that is, in  
22     the case of reading the unencrypted data). On the contrary,  
23     if the value of the flag bit 1403 is set to "1" (that is, in  
24     the case of reading the encrypted data), the read-out data  
25     are decrypted.

26          In the example shown in Fig. 16A, the sector data 1402  
27     corresponding to the sector numbers "0" and "2" are read out  
28     and new data are written in the sector number "0". In this  
29     event of data writing, the sector data 1402 being written  
30     are encrypted and the value of the corresponding flag bit  
31     1403 is set to "1". Meanwhile, in the example shown in Fig.

1 16B, the sector data 1402 corresponding to the sector  
2 numbers "0" and "2" are read out and new data are written  
3 therein. The sector data 1402 in the sector number "0" are  
4 encrypted upon writing as shown in Fig. 16A. Accordingly,  
5 the sector data 1402 therein are decrypted upon reading. In  
6 addition, both of the sector data 1402 to be newly written  
7 in the sector numbers "0" and "2" are encrypted, whereby the  
8 values of the corresponding flag bits 1403 are set to "1".

9 Fig. 17 is a view showing aspects of the sector data  
10 1402 and the flag bits 1403 when data reading and writing is  
11 executed in the state where the encryption function of the  
12 hard disk device 100 is once turned on and then turned off  
13 again.

14 In this case, the sector data 1402 written in the  
15 state of turning on the encryption function are encrypted.  
16 Accordingly, the relevant sector data 1402 are decrypted  
17 upon reading. Meanwhile, the unencrypted sector data 1402  
18 are read out directly. The sector data 1402 to be newly  
19 written after setting the encryption function to an  
20 off-state are not encrypted, whereby the values of the  
21 corresponding flag bits 1403 are set to "0".

22 In the example shown in Fig. 17, the sector data 1402  
23 corresponding to the sector numbers "0" and "2" are read out  
24 and new data are written therein. In this event, the  
25 encrypted sector data 1402 in the sector number "0" are  
26 decrypted upon reading. In the meantime, no encryption is  
27 executed upon writing.

28 In this way, the encryption and decryption processing  
29 is executed in response to the turning on and off of the  
30 encryption function of the hard disk device 100 every time  
31 of data writing and reading in and out of each sector.

1 Here, as described in the chapter "A. Processing concerning  
2 management of an encryption key", in the case of executing  
3 the user verification by use of the personal identification  
4 information such as a password, the verification is executed  
5 when the encryption function is set to an on-state so as to  
6 use the encryption key, and the encryption key is made  
7 usable without the verification when the encryption function  
8 is set to an off-state (by means of saving the unencrypted  
9 encryption key in the magnetic disk 10 as described in the  
10 operation 7, for example). In this way, when the encryption  
11 function is turned off, the sector data 1402 are automati-  
12 cally decrypted upon reading if the corresponding flag bit  
13 1403 is set to "1". Accordingly, the user can read and  
14 write the data without recognizing as to whether the read-  
15 out data has been encrypted or not.

16 Here, when the single hard disk device 100 is shared  
17 by a plurality of users, the management of the encryption  
18 processing for each sector by user can be executed if it is  
19 possible to prepare a plurality of flag bits 1403 for each  
20 sector.

21 In the above-described control for encryption and  
22 decryption of the stored data, the CBC mode is applied as  
23 the use mode for encryption. Moreover, the sector number is  
24 used as the initial vector and the pseudo-random number  $C_{IV}$   
25 obtained by encrypting the initial vector is initially  
26 applied upon encrypting the stored data. However, confiden-  
27 tiality is not required in the initial vector or the pseudo-  
28 random number  $C_{IV}$  obtained by encrypting the initial vector,  
29 and arbitrary values can be used therein. Moreover, the  
30 sector number is a value uniquely allotted to each sector.  
31 Accordingly, it is possible to obtain the ciphertext block,

1 which are different from one another depending on the  
2 sectors, even if the sector numbers are directly used for  
3 encrypting the same data without conversion into random  
4 numbers. Therefore, it is also possible to execute the  
5 initial encryption by means of subjecting the sector number  
6 directly to the XOR operation with the plaintext block  $P_0$ .

7 As described above, in this embodiment, the encryption  
8 circuit 54 is incorporated into the hard disk controller 50  
9 of the hard disk device 100. Accordingly, it is possible to  
10 execute the encryption processing of the stored data in the  
11 hard disk device 100 without executing special processing on  
12 the side of the computer device (the OS) being the host  
13 system, in other words, without recognition by the user.

14 Moreover, the data encryption key for use in the  
15 encryption processing of the stored data is encrypted with  
16 another encryption key created out of the personal identifi-  
17 cation information, and the encrypted data encryption key is  
18 stored in the magnetic disk 10. Accordingly, it is possible  
19 to deal with a change in the personal identification infor-  
20 mation just by re-encrypting the data encryption key. In  
21 this way, it is unnecessary to perform a complicated opera-  
22 tion of decrypting the entire stored data and then  
23 re-encrypting the stored data again.

24 Furthermore, execution of the data encryption process-  
25 ing by each unit for reading and writing the stored data,  
26 such as the sector, is controlled in response to the turning  
27 on and off of the encryption function of the hard disk  
28 device 100. Accordingly, encryption or decryption of the  
29 stored data can be performed without allowing the user to  
30 recognize such an operation upon data access. For this  
31 reason, it is possible to mix the encrypted stored data and



1 the unencrypted stored data together in the magnetic disk 10  
2 comfortably. Therefore, it is unnecessary to perform a  
3 complicated operation of encrypting or decrypting the entire  
4 stored data every time when the encryption function is  
5 turned on or off. In addition, when certain software is  
6 preinstalled in the hard disk device 100 (or in the computer  
7 device) upon shipment, it is possible to realize the follow-  
8 ing using method easily, in which the software is kept  
9 unencrypted in the initial state of shipment because the  
10 software does not require confidentiality, and then the data  
11 written or read out after the encryption is turned on by the  
12 user are encrypted because the data is deemed to require  
13 confidentiality. Meanwhile, when it is necessary to encrypt  
14 the entire data stored in the magnetic disk 10 after turning  
15 on the encryption function, the entire data or the enter  
16 sectors may be serially read out and encrypted and rewritten  
17 after the encryption. In this way, although the processing  
18 requires some time, it is still possible to encrypt the  
19 entire data.

20 Note that the foregoing embodiment has been described  
21 while targeting on the hard disk device 100 including the  
22 magnetic disk as the recording medium. However, the present  
23 invention is also applicable to encryption processing for  
24 data writing and reading in and out of various external  
25 storage devices which adopts various recording media,  
26 including, optical discs such as a digital versatile disc  
27 (DVD) or a compact disc, memory cards, and the like.

28 Moreover, the foregoing embodiment has been described  
29 regarding the case of using the symmetric key cipher as the  
30 encryption method while considering the convenience for  
31 encrypting the write data and decrypting the read data.

1 However, the encryption method for encrypting the stored  
2 data and the personal identification information is not  
3 necessarily limited to the common key encryption. For  
4 example, it is also possible to use public key cipher upon  
5 encrypting the personal identification information or the  
6 like, which does not need to be decrypted from the verifica-  
7 tion data into the original data in the event of executing  
8 the user verification.

9 Furthermore, the encryption processing according to  
10 the above-described embodiment is particularly suitable for  
11 the case where the encryption processing of the stored data  
12 is controlled not by the host system but by the external  
13 storage device itself and where the encryption processing  
14 and the user verification are executed at the same time.  
15 However, it is obvious that there is another possibility of  
16 an embodiment, in which the encryption processing and the  
17 user verification are executed under control of the host  
18 system. In this case, the encryption processing and the  
19 user verification will be executed by use of a program-  
20 controlled CPU of a computer device being the host system,  
21 or by use of the CPU and a given encryption circuit as the  
22 encryption processing means.

23 As described above, according to the present  
24 invention, it is possible to achieve the encryption process-  
25 ing of the stored data and management of the encryption key,  
26 which are suitable for the case when the user verification  
27 and encryption of the stored data are applied to a storage  
28 device at the same time.

29 Moreover, according to the present invention, it is  
30 possible to provide the method of encryption processing for  
31 the stored data suitable for the detachably implemented

1 storage device, and to provide the storage device which can  
2 achieve the method of encryption processing.

3 Although advantageous embodiments of the present  
4 invention have been described in detail, it should be under-  
5 stood that various changes, substitutions, and alternations  
6 can be made therein without departing from spirit and scope  
7 of the inventions as defined by the appended claims.

8 Variations described for the present invention can be  
9 realized in any combination desirable for each particular  
10 application. Thus particular limitations, and/or embodiment  
11 enhancements described herein, which may have particular  
12 advantages to a particular application need not be used for  
13 all applications. Also, not all limitations need be imple-  
14 mented in methods, systems and/or apparatus including one or  
15 more concepts of the present invention.

16 The present invention can be realized in hardware,  
17 software, or a combination of hardware and software. A  
18 visualization tool according to the present invention can be  
19 realized in a centralized fashion in one computer system, or  
20 in a distributed fashion where different elements are spread  
21 across several interconnected computer systems. Any kind of  
22 computer system - or other apparatus adapted for carrying  
23 out the methods and/or functions described herein - is  
24 suitable. A typical combination of hardware and software  
25 could be a general purpose computer system with a computer  
26 program that, when being loaded and executed, controls the  
27 computer system such that it carries out the methods  
28 described herein. The present invention can also be embed-  
29 ded in a computer program product, which comprises all the  
30 features enabling the implementation of the methods  
31 described herein, and which - when loaded in a computer

1 system - is able to carry out these methods.

2 Computer program means or computer program in the  
3 present context include any expression, in any language,  
4 code or notation, of a set of instructions intended to cause  
5 a system having an information processing capability to  
6 perform a particular function either directly or after  
7 conversion to another language, code or notation, and/or  
8 reproduction in a different material form.

9 Thus the invention includes an article of manufacture  
10 which comprises a computer usable medium having computer  
11 readable program code means embodied therein for causing a  
12 function described above. The computer readable program  
13 code means in the article of manufacture comprises computer  
14 readable program code means for causing a computer to effect  
15 the steps of a method of this invention. Similarly, the  
16 present invention may be implemented as a computer program  
17 product comprising a computer usable medium having computer  
18 readable program code means embodied therein for causing a a  
19 function described above. The computer readable program  
20 code means in the computer program product comprising  
21 computer readable program code means for causing a computer  
22 to effect one or more functions of this invention. Further-  
23 more, the present invention may be implemented as a program  
24 storage device readable by machine, tangibly embodying a  
25 program of instructions executable by the machine to perform  
26 method steps for causing one or more functions of this  
27 invention.

28 It is noted that the foregoing has outlined some of  
29 the more pertinent objects and embodiments of the present  
30 invention. This invention may be used for many  
31 applications. Thus, although the description is made for

1 particular arrangements and methods, the intent and concept  
2 of the invention is suitable and applicable to other  
3 arrangements and applications. It will be clear to those  
4 skilled in the art that modifications to the disclosed  
5 embodiments can be effected without departing from the  
6 spirit and scope of the invention. The described embodi-  
7 ments ought to be construed to be merely illustrative of  
8 some of the more prominent features and applications of the  
9 invention. Other beneficial results can be realized by  
10 applying the disclosed invention in a different manner or  
11 modifying the invention in ways known to those familiar with  
12 the art.